Міністерство освіти і науки України
Вінницький національний технічний університет

Матеріали LI науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2022)

31 травня 2022 року

Збірник доповідей

Електронне наукове видання

Вінниця
ВНТУ
2022

УДК 001
М34

Видається за рішенням Вченої ради Вінницького національного технічного університету Міністерства освіти і науки України

Головний редактор: В. В. Біліченко
Відповідальний за випуск: В. В. Грабко

Робоча група з підготовки конференції:
Голова робочої групи:
проректор з наукової роботи та міжнародного співробітництва ВНТУ В. В. Грабко;

Члени робочої групи:

декани факультетів, директор Інституту Конфуція ВНТУ;

Власюк А. І., начальник РВВ, доц.;

Могила С. Г., інженер 1-ї категорії РВВ;
Сідак С. Г., редактор РВВ;
Тамтура Я., О. редактор РВВ.

М34 **Матеріали** LI науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2022) : збірник доповідей [Електронний ресурс]. – Вінниця : ВНТУ, 2022. – (PDF, 2830 с.)
ISBN 987-966-641-894-7

Збірник містить тексти доповідей LI ювілейної регіональної науково-технічної конференції професорсько-викладацького складу, науковців, аспірантів та студентів Вінницького національного технічного університету з участю працівників підприємств м. Вінниці та Вінницької області з загально-інженерних, технічних, гуманітарних та фундаментальних наук.

НТКП ВНТУ проводиться у вигляді конференцій факультетів та конференції Інституту Конфуція ВНТУ. Кожна конференція має власну тематику, оргкомітет, строки проведення пленарних та секційних засідань, та складається з однієї або кількох секцій.

УДК 001

ISBN 978-966-641-894-7

УДК 004.7

П. П. Малініч
І. П. Малініч
О. О. Коваленко

Негативні безпекові чинники у локальних Ethernet-мережах та абонентських мереж останньої милі

Вінницький Національний технічний університет

Анотація
Сучасні провайдери послуг фіксованого доступу до мережі Інтернет, а також компанії з великими локальними мережами однаково є зацікавленими над оптимізацією витрат на закупку мережевого обладнання. Кожна компанія визначає свій власний баланс між більш дешевими апаратними мережевими рішеннями з обмеженим функціоналом та більш дорогими, які дають більше контролю над безпековим периметром мережі. Представлений аналіз у більшій мірі триматиме фокус на мережах які використовують більш дешеві апаратні рішення на базі бюджетних маршрутизаторів та комутаторів, де наявні лише найбільш базові захисту для захисту на кшталт фільтрації та основі MAC-адрес, а також розглядатимуться можливі напрямки для розвитку їх захищеності без збільшення вартості апаратного забезпечення.
Ключові слова: комп'ютерні мережі, маршрутизатори, комутатори, безпека, бюджетні мережеві рішення

Abstract
Nowadays ISP's of fixed Internet access services, as well as companies with large local area networks are equally interested in optimizing the budget of purchasing network equipment. Each company determines its own balance between cheaper hardware networking solutions with limited functionality and more expensive ones that give more control over the secure perimeter of the network. This review will be more focused on networks that use cheaper hardware solutions based on budget routers and switches, where only the most basic protections are available for protection such as filtering and MAC addresses, and will consider possible ways to develop their security without increasing the cost of hardware.
Keywords: computer networks, routers, switches, security, small business network solutions

Вступ

Нині існує чимало вразливостей у різних програмних продуктах та мікропрограмах різних пристроїв, однак не менш критичними є безпекові проблеми у мережевій інфраструктурі. Питання безпеки фізичних комп'ютерних мереж є більш комплексним, оскільки майже завжди охоплює більше ніж один пристрій. Найбільш популярні дослідження з цієї теми [1-5] умовно відносять безпекові ризики Ethernet-мереж на як мінімум до двох категорій: ті, для виникнення яких потрібен фізичний доступ зі сторони недоброзичників, та інші, які можуть виникати без безпосереднього фізичного доступу. Мережеві атаки з отриманням фізичного дають значно більші можливості для порушення роботи мережі, полегшують доступ до внутрішніх ресурсів мережі, а також можуть дати змогу перехоплювати трафік, однак є більш складними для виконання і трапляються рідше.

Існує досить багато рішень захисту мереж корпоративного класу [5], які наприклад використовуються банками, медичними закладами, а також великим бізнесом, однак в даному

матеріалі більше уваги приділяється мережам початкового рівня та мережевим рішенням для малого бізнесу.

Огляд безпекових чинників у Ethernet-мережах

Атаки, для яких фізичний доступ не є обов'язковим, і які можуть вестись віддалено є найбільш універсальними і до них різного роду зловмисники вдаються більш часто, оскільки атаки з отриманням фізичного доступу є надзвичайно рідкісними. Причиною тому слугує те, що вони є невиправдано затратними і нерідко дуже складними.

До безконтактних атак в сенсі відсутності необхідності у безпосередньому фізичному зв'язку можна віднести DDoS-атаки. Звісно, на перший погляд може здаватись що DDoS-атаки на мережі що лише забезпечують Інтернет-доступ провести значно складніше, однак відомі випадки з мережами за NAT-бар'єром [6], коли за допомогою подібних DDoS-атак уповільнився Інтернет-зв'язок та зменшилась його якість. Мережі за NAT-бар'єром можуть бути також вразливі до атак на виснаження ресурсів, оскільки кількість NAT-сесій обмежується кількістю білих IP-адрес, а також обчислювальними ресурсами.

Серед більш продвинутих способів втручання з працюючих дистанційно у локальних мережах та мережах останньої милі можна виділити наступні: можливість сканування мережі, взлами хостів, віддалений доступ до мережі, а також можливість керування комутатором. Сканування мережі є переважно можливим у випадках, коли NAT не використовується або при недостатньо захищеній конфігурації протоколу IPv6. Сканування мережі також стає доступним у сценаріях, якщо один із хостів мережі є взломаним, або якщо зловмисник зміг іншим чином отримати віддалений доступ до мережі [1]. Віддалений доступ може бути отриманий при компрометації одного із вже існуючих способів віддаленого мережевого доступу, таких як корпоративний VPN-доступ. Однак подібний доступ може бути створеним і при отриманні контролі над певним хостом, що дозволить не лише створити канал між зловмисником та цільовою мережею, що у свою чергу дозволить використовувати і більш специфічні інструменти для збору даних та впливу на процеси у комп'ютерній мережі. Дистанційне отримання контролю над комутатором є теж можливим [5], особливо у випадках коли засоби керування ним (SSH, Telnet, SNMP чи веб-панель) стають доступними для тих, хто хотів би цим скористатись. Однак можливості програмного забезпечення прошивки керуємих комутаторів не завжди можуть створити достатньо можливостей для перехоплення або зміни трафіку - тому при несанкціонованому доступі до даного виду пристроїв найбільш ймовірно виникне ризик припинення досутпу до ресурсів, які залежать від роботи подібного пристрою.

Наявність фізичного доступу до мережевої інфраструктури суттєво збільшує можливості зловмисників для взлому більшої кількості пристроїв у мережі. В сучасних реаліях безпосередній фізичний доступ до корпоративних локальних мереж зі сторони зловмисників є не зовсім можливим, але подібний доступ може мати місце у вигляді підключень через погано захищений WiFi, через інфікування пристроїв співробітників або серверів, які мають змогу підключитись до корпоративної мережі. Особливу небезпеку можуть становити погано захищені сервери віртуалізації, в яких у віртуальних машин присутня можливість безпосереднього з'єднання із L2-мережею. Тоді може значно зрости можливість виникнення атак на L2-рівні, таких як MITM-атаки та отруєння ARP і DHCP.

Досить великий ризик зіткнутись із повністю справжнім фізичним несанкціонованим доступом є у провайдерів доступу до мережі Інтернет, для яких насамперед важливо вберегтись від проявів

недобросовісної конкуренції та спроб самовільно підключитись зі сторони недобросовісних жителів. Як результат існують наступні можливі види взлому [4]:

- несанкціоноване приєднання;
- несанкціоноване розширення мережі;
- тегування та перехід VLAN;
- приєднання до VLAN;

Можливості підвищення захищеності низькобюджетних мереж

Серед найбільш універсальних рішень для підвищення захищеності низькобюджетних комп'ютерних мереж є такі: ізоляція гостьових WiFi-мереж, використання маршрутизаторів з налаштовуємим фаєрволом; розподіл різних підмереж на різні класи довіри. Серед більш продвинутих рішень знаходяться системи виявлення вторгнень (IDS) та системи моніторингу системних журналів.

Обидва зазначених рішення потребують підвищення вартості та функціоналу обладнання. Звісно без цього не вийде захиститись від більш складних атак, однак також існують методи моніторингу мережі на базі сканувальних технологій, які дозволяють виявляти зміни у піднятих мережевих сервісах важливих хостів, а також виявляти підозрілі хости у високопріоритетних мережах. Подібний функціонал присутній у програмному пакеті Trend Micro Deep Discovery Inspector [7], але на даний момент в специфікації не описано прикладів застосування без централізованого журналювання та з використанням низькобюджетної мережевої інфраструктури. Само тому є більш очевидною необхідність більш детально дослідити можливості для моніторингу захищеності мережевих сервісів та виявлення підозрілих хостів.

Висновки

Нині існує досить багато потенційних безпекових загроз для низькобюджетних комп'ютерних мереж - як повністю віртуальних, так і таких, що пов'язані з фізичним втручанням. Існує чимало технологій для виявлення вторгнень та моніторингу захищеності сервісів, однак не всі з них можливо використати у низькобюджетних комп'ютерних локальних мережах та абонентських мережах останньої милі. Саме тому є сенс дослідити можливість їх застосування у подібних мережах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kiravuo, T., Sarela, M. and Manner, J., 2013. A survey of Ethernet LAN security. IEEE Communications Surveys & Tutorials, 15(3), pp.1477-1491.
2. Wahid, K.F., 2010, April. Maximizing Ethernet security by switch-based single secure domain. In 2010 Seventh International Conference on Information Technology: New Generations (pp. 774-778). IEEE.
3. Guruprasad, A., Pandey, P. and Prashant, B., 2003, October. Security features in Ethernet switches for access networks. In TENCON 2003. Conference on Convergent Technologies for Asia-Pacific Region (Vol. 3, pp. 1211-1214). IEEE.
4. Wahid, K.F., 2010, May. Rethinking the link security approach to manage large scale Ethernet network. In 2010 17th IEEE Workshop on Local & Metropolitan Area Networks (LANMAN) (pp. 1-6). IEEE.
5. Vyncke, E. and Paggen, C., 2007. Lan switch security: what hackers know about your switches. Cisco Press.
6. The Effect of DDoS Attacks on Carrier-grade NAT Devices. Url: https://www.a10networks.com/resources/videos/the-effect-of-ddos-attacks-on-carrier-grade-nat-devices/
7. Trend Micro Deep Discovery Inspector Online. URL:https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/inspector.html/

Малініч Павло Павлович, ст. гр. 1ПІ-18б, Факультет інформаційних технологій та комп'ютерної інженерії, м. Вінниця, pavlo.malinich@vntu.edu.ua

Малініч Ілля Павлович, асистент каф. КН
Коваленко Олена Олексіївна, к.т.н., доц. каф. ПЗ

Malinich Pavlo Pavlovych, student of 1PI-18b group, Faculty of Information Technologies and Computer Engineering, Vinnytsia, pavlo.malinich@vntu.edu.ua
Malinich Illia Pavlovich, assistant of the department CN
Kovalenko Olena Oleksiivna, Candidate of Technical Sciences, docent of kaf. Software